GDPR

What is the GDPR?

The EU's General Data Protection Regulation 2016/679 (GDPR) is a regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area. This regulation is applicable to all organisations that hold personal data.

In the United Kingdom, GDPR will supersede the Data Protection Act 1998, which was brought into law as a way to implement the 1995 EU Data Protection Directive. GDPR seeks to give people more control over how organisations use their data, and introduced strict fines for organisations that fail to comply with the rules, and for those that suffer data breaches. This regulation also ensure that across the EU data protection laws are identical.

When will the GDPR come in to effect?

The GDPR will come into effect on the 25 May 2018. As GDPR is a regulation and not a directive, the UK does not need to draw up new legislation, instead it will automatically apply.

Who does the GDPR apply to?

The GDPR applies to 'Controllers' and 'processors' of data. The controller says how and why personal data is processed and the processer acts on the controllers behalf of actually processing the data. A controller can be any type of organization from a charity (non-profit) organization, government or profit making company. A processor could be an external company such as an IT business that looks after and processes the data.

The GDPR rules will still apply to controllers and processers even if they are based outside the EU as long as they are dealing with EU residents data.

It is the controller's responsibility to ensure their processor abides by data protection laws and processors must also abide by the rules to maintain records of their data processing activities. If there is a data breach the processor is far more liable under the GDPR than under the old Data Protection Act.

When can data be processed under the GDPR?

Once the legislation comes into effect on the 25 May 2018, controllers must ensure that all personal data is processed lawfully, transparently and for a clear specific purpose. All data should be deleted once that purpose has been fulfilled and the data is no longer required.Guide to the General Data Protection Regulation If you wish to find out more about GDPR, please go to the Information Commissioners Office website at www.ico.org.uk for more information.